APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,728	10/31/2001	Richard Paul Tarquini	10017270-1	3625

7590   03/24/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Jレ

	Application No..	Applicant(s)
Office Action Summary	10/001,728	TARQUINI ET AL.
	Examiner	Art Unit	
	Samson B Lemma	2132	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _31 October 2001_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-13_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-13_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _JUL,28,2003_.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

1. **Claims 1-13** have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form

the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1 and 3-10** are rejected under 35 U.S.C. 102(e) as being anticipated by **Victor**

Kouznetsov (hereinafter referred as **Kouznetsov**) (U.S. Patent No 6,725,377B1)

4. **As per claim 1 and 9-10, Kouznetsov** a mobile device operable in a mobile

telecommunications network, comprising:

- **A memory module for storing data in machine readable format for retrieval**

  and execution by a central processing unit; [Column 1, lines 53-55;column 4,

  lines 43-47; column 4, lines 63-65; column 6, lines 58-61; column 10, lines 19-

  22] (The anti-intrusion software program which is stored on the CD-ROM or

  floppy disk is installed on any computer/server by the system administrator as

  explained on column 4, lines 43-47 and column 4, lines 53-55 and the system

  administrator is required to retrieve and install the latest versions of updates for

each servers. Therefore, inherently, this program is installed in the computers

memory and any computer larger or small, must have a central processing unit

for execution of this software program installed in its memory module.)

- **An operating system operable to execute an intrusion detection application**

  stored in the memory module.[Column 6, lines 32-34;column 7, lines 46-

  48;column 2, lines 39-41] (First as explained on column 2, lines 25-26 and

  column 2, lines 32-35 it has been disclosed that the **CyberCop Network** which

  is the real time intrusion detection application software is offered in a variety of

  outlets and forms. It is accompanied by documentation including the **CyberCop**

  Network for windows NT version 2 **operating system**. The anti-intrusion

  monitor server which has stored the intrusion application software manually by

  the administrator in its own memory module as explained on column 4, lines

  43-47, performd program execution using Pentium based server running

  Window NT operating system as explained on column 6, lines 32-34].

5.   **As per claim 3**, **Kouznetsov** discloses the device as applied to claim 1 above.

Furthermore **Kouznetsov** discloses the device wherein the intrusion detection

application further comprises an associative process engine and an input/output

control layer, the input/output control layer operable to receive a signature file and

pass the signature file to the associative process engine, the associative process engine

operable to analyze a data packet with the signature file. [Figure 2, column 7, lines 31-

38] (The intrusion application which is first loaded at central anti-intrusion server

shown at figure 5, ref. Num "514" transmits the modified attack/pattern or signature

file to the push administration and the push administration transmit the modified

attack/pattern or signature to the anti-intrusion server shown on figure 2, ref. Num

"202" meets the recitation of the claim.)

6.   **As per claim 4, Kouznetsov** discloses the device as applied to claim 1 above.

Furthermore **Kouznetsov** discloses the device further comprising a storage media, the

storage media operable to maintain a database of a plurality of signature files

therein.[column 7, lines 62-67]

7.   **As per claims 5-8, Kouznetsov** discloses the device as applied to claims above.

Furthermore **Kouznetsov** discloses the device wherein the intrusion detection

application identifies a correspondence between the signature file and a data packet, a

determination that the data packet is intrusion-related made upon identification of the

correspondence. [Column 7, lines 31-38]

Claim Rejections - 35 USC § 103

8.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as
> set forth in section 102 of this title, if the differences between the subject matter sought to be
> patented and the prior art are such that the subject matter as a whole would have been obvious
> at the time the invention was made to a person having ordinary skill in the art to which said
> subject matter pertains. Patentability shall not be negatived by the manner in which the
> invention was made.

9.   **Claims 11-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Holland**

III et al (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061) in view of **Smaha**

et al, (hereinafter referred to as **Smaha**) (U.S. Patent No. 5,557,742)

10.   **As per claims 11-13**, Holland discloses **a node** [figure 1, ref. Num "11"' ref. Num "12"]

of a **network for managing an intrusion detection system,**[Column 1, lines 15-18;

figure 1, ref. Num "20", ref. Num "19", ref. Num 18"] (The present invention relates in

general to network intrusion detection data collection and, in particular, to a system

and method for intrusion detection data collection using a network protocol stack

multiplexor). **The node comprising**:

- **A memory module for storing data in machine readable format for retrieval and execution by the central processing unit**; [Column 4, lines 23-29]

  - **An operating system** [Figure 2, ref. Num "Kernel"] (The Kernel is the core of an operating system such as Windows 98, Windows NT, Mac OS or Unix. Provides basic services for the other parts of the operating system, making it possible for it to run several programs at once multitasking, read and write files and connect to networks and peripherals.) **comprising**

    A network stack comprising a protocol driver,[Figure 1, ref. Num "33"; figure 3, ref. Num "52"; figure 4, ref. Num "82" and ref. Num "83"; Column 6, lines 27-31] (The protocol driver is inherently included in the IP stack since, in the network architecture used in windows 2000 and later the LLC, network and transport layer which are part of the IP layer shown on figure 4, ref. Num "82", "83" are implemented by software drivers which are also called protocol drivers) and

  - **A media access control driver** [figure 2, ref. Num "31"; column 4, lines 53-57] (The MAC driver or media access control driver is also inherently included in the NIC. The MAC or the "media access control driver", also called the network card driver, allows the operating system to talk with the NIC. Windows NT and Windows 95/98 come with MAC drivers for most NICs. The MAC driver got its name from the fact that it operates at the lower level of the

OSI model. The second layer of the model, the Data Link layer, is divided into

two pieces: the LLC and MAC. The LLC sub layer is implemented in the

transport driver while the MAC sub layer is implemented in the NIC) and

operable to execute an intrusion protection system [Column 4, Lines 52-

53;figure 2, ref. Num "37" and column 4, lines 31-32]

Holland does not explicitly discloses

- Management application, the management application operable to

receive text-file input defining a network-exploit rule and convert the text-file

input into a signature file comprising machine-readable logic representative of

an exploit-signature, the node operable to transmit the signature file to a mobile

device over a radio frequency link.

However, in the same field of endeavor, **Smaha** discloses

An application operable to receive text-file input defining a network-exploit

[figure 1, ref. Num "20" and "12"; figure 5a, ref.Num "12"; column 4, lines 40-49]

(For instance, input mechanism shown on figure 1, ref. Num "20" receives input

from any wide array of sources for example user devices shown on figure 1, ref.

Num "22") and **convert the text-file input into a signature file comprising**

machine-readable logic representative of an exploit-signature, [figure 5a,

ref. Num "144"; column 5, lines 10-12; Column 6, lines 9-11] (The misuse

engine shown on figure 1, ref. Num "30" converts the input into

events/signature and compare it with the known signatures and generate a

signature representative of an exploit-signature when detecting a misuse during

processing operations and send it to the out put mechanism as shown on figure

5a, ref. Num "32") and **the node operable to transmit the signature file to a**

radio frequency link.[column 6, lines 15-17; figure 1, ref. Num "36" and "38"
and ref. Num "40"] (the output signal is sent to the communication links.)

It would have been obvious to one having ordinary skill in the art,
at the time the invention was made, to combine the features of
converting the input into events/signature and compare it with
the known signatures and generate a signature representative of
an exploit-signature when detecting a misuse during processing
operations and send it to the out put mechanism as shown on
figure 5a, ref. Num "32" and transmitting to the communication
links as per teachings of **Smaha** in to the method of analyzing the
traffic using signature-based and statistical-based intrusion
detection techniques as taught by **Holland**, in order to create a
system a system capable of automatically recognizing intrustions
and misuses.(See Smaha, Column 3, lines 9-10)

11.   **Claims 2** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Victor
Kouznetsov** (hereinafter referred as **Kouznetsov**) (U.S. Patent No 6,725,377B1)
in view of Holland III et al (hereinafter referred as **Holland**) (U.S. Patent No 6,851,061)

12.   As per claim 2, **Kouznetsov** discloses a device or a method of monitoring intrusion
using an anti-intrusion monitor server running Window NT operating system. [Column
6, lines 32-34]

Kouznetsov does not explicitly discloses

* The operating system further comprises a network stack comprising a protocol
driver, a media access control driver, the intrusion detection application comprising an
intermediate driver bound to the protocol driver and the media access control driver.

However, in the same field of endeavor, **Holland** discloses

An operating system [Figure 2, ref. Num "Kernel"] (The Kernel is the core of an

operating system such as Windows 98, Windows NT, Mac OS or Unix. Provides

basic services for the other parts of the operating system, making it possible for

it to run several programs at once multitasking, read and write files and connect

to networks and peripherals.) **comprising**

A network stack comprising a protocol driver,[Figure 1, ref. Num "33"; figure

3, ref. Num "52"; figure 4, ref. Num "82" and ref. Num "83"; Column 6, lines 27-

31] (The protocol driver is inherently included in the IP stack since, in the

network architecture used in windows 2000 and later the LLC, network and

transport layer which are part of the IP layer shown on figure 4, ref. Num "82",

"83" are implemented by software drivers which are also called protocol drivers)

• **A media access control driver** [figure 2, ref. Num "31"; column 4, lines

53-57] (The MAC driver or media access control driver is also inherently

included in the NIC. The MAC or the "media access control driver", also called

the network card driver, allows the operating system to talk with the NIC.

Windows NT and Windows 95/98 come with MAC drivers for most NICs. The

MAC driver got its name from the fact that it operates at the lower level of the

OSI model. The second layer of the model, the Data Link layer, is divided into

two pieces: the LLC and MAC. The LLC sub layer is implemented in the

transport driver while the MAC sub layer is implemented in the NIC) and

• **The intrusion detection system implemented as an**

intermediate driver [Figure 2, ref. Num "37"] and bound to

the protocol driver [figure 2, ref. Num "33"] and **the media**

access control driver.[figure 2, ref. Num "31"] (With respect to **Holland** the Packet filter/an instance of the intrusion detection service which is shown on figure 2, ref. Num "37" is implemented as an intermediate driver and bound to the MAC driver which is inherently included in the NIC and to the protocol driver which is inherently included in the IP stack shown on figure 2, ref. Num "33" and shown also on figure 3, ref. Num "52. This is because the IP protocol stack implementation disclosed on column 6, lines 27-31 and particularly shown on figure 4, ref. Num "82" and "83", namely the network layer and the transport layer are all implemented by the protocol driver.)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of the operating system as per teachings of **Kouznetsov** in to the method of operating system which comprises the network stack as taught by **Holland**, in order to relates network intrusion detection with respect to a network protocol stack.

Conclusion

13.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).
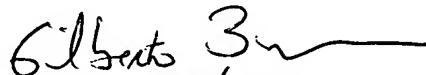
If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone

number for the organization where this application or proceeding is assigned is 703-872-

9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information

for unpublished applications is available through Private PAIR only. For more information

about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on

access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-

217-9197 (toll-free).

SAMSON LEMMA
S·L·
03/10/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100